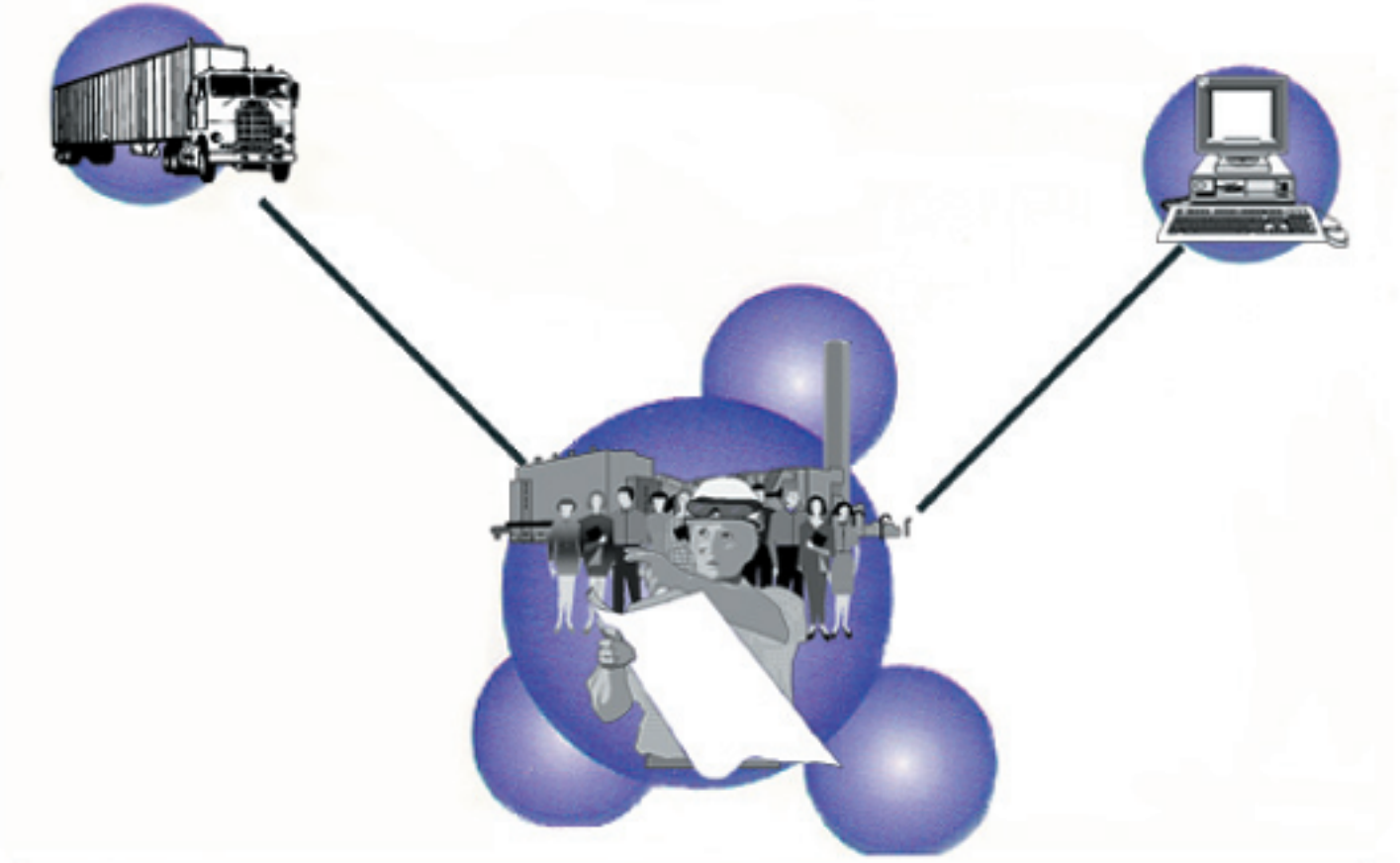
EPA 550-F-99-011
June 1999

Addressing Year 2000 Issues in Small and Medium-Sized Facilities that Handle Chemicals



Addressing Year 2000 Issues in Small and Medium-Sized Facilities That Handle Chemicals

Several chemical industry trade associations[1] representing manufacturers, formulators, distributors and retailers - in partnership with the U.S. Chemical Safety and Hazard Investigation Board (CSB) and the U.S. Environmental Protection Agency (EPA) - are issuing this document as part of an ongoing effort to assess and address potential Y2K disruptions in facility operations, particularly safety-related control systems and equipment. This document is offered as a public service, and it is oriented toward owners and operators of small and medium-sized entities.

The statements in this document are intended solely as guidelines. Site-specific application of these guidelines may vary depending on process activities and unique facility characteristics. Source material used to develop this document was produced by the United Kingdom's Health and Safety Executive, the U.S. CSB , EPA. And

[1]Participating organizations: the American Crop Protection Association, the Chemical Manufacturers Association, the Chemical Producers and Distributors Association, the Chemical Specialties Manufacturers Association, the International Sanitary Supply Association, the National Association of Chemical Distributors, RISE (Responsible Industry for a Sound Environment), and the Synthetic Organic Chemical Manufacturers Association.

Introduction

Many systems and pieces of equipment used to sustain process safety in chemical facilities rely on the progression of dates from year to year (for example, 1998 to 1999) to function properly. This includes not only mainframe and personal computers, but also any equipment that contains a microchip such as heating, lighting, safety, and telecommunications systems. Many of these systems "read" only the last two digits of the year - 1998 becomes "98," 1999 becomes "99." As a result, they may be vulnerable to problems when the year 2000 (Y2K) begins, because they cannot recognize that "00" means 2000, not 1900. This can cause problems at any level of the system - the clock, the Basic Input/Output System (BIOS), the operating system, the application software, or even the data itself. Y2K failures external to your facility, such as disruptions in electricity, water and transportation, may also affect your facility's operation.

This document describes a five-step process for protecting the continuity of the process safety systems in your facility from potential Y2K problems. Additionally, the appendices contain information to help you throughout the process. This document includes the following:

- A checklist of typical in-plant systems potentially vulnerable to Y2K disruptions to help you determine where to focus

your efforts ***(Appendix A)***

- Guidelines for assessing the effect on safety and deciding priorities ***(Appendix B)***
- Sources for obtaining Y2K resource material ***(Appendix C)***
- A list of specific key dates that may cause disruptions ***(Appendix D)***
- A guide for communicating your activities to your employees and your community ***(Appendix E)***

Step 1 - Assessment

The first step in the process is to conduct an assessment to gather the information you need to ensure that you can protect safety systems and equipment. Begin by conducting a thorough inventory to identify all systems, computerized equipment, and devices with embedded computer chips that may be vulnerable to date-change failure. This includes systems that import and/or export data and should take into account systems with which they exchange data. ***Appendix A*** has a checklist that includes systems that may have embedded chips or are susceptible to a Y2K disruption. Also, ***Appendix B*** has a checklist ***(Figure 2)*** you can use to help you determine if a system or device is date-dependent.

For each item, define the extent of work necessary for Y2K compliance. In some cases, this can be accomplished by referring to user manuals and other documentation provided with the equipment. In other cases, it may involve contacting suppliers to obtain needed information. Determine whether or not the supplier believes the system, as supplied, is "year 2000 compliant," - that is, able to accommodate the transition to Y2K and correctly continue date-based calculations. It is important to obtain satisfactory written assurance of compliance from the supplier whenever possible. Such assurance may be sufficient for some systems that are being used as supplied and that have a low safety risk.

For systems and equipment that are not Y2K compliant, manufacturers or suppliers may be able to provide assistance with making the required changes. In some cases, however, you may be unable to obtain this kind of help. Hardware or software for some systems and equipment may have been changed or adapted for use in your facility, and these changes could affect the ability of the system to correctly make date changes and date-based calculations. You may be using equipment and software that no longer is supported by a supplier or by the original manufacturer. The supplier may be unable to provide immediate assistance because of current workload; ownership of the business may have changed hands; or the manufacturers or suppliers may have gone out of business entirely. In these circumstances, your options for dealing with systems and equipment will depend on the amount of information available, the other resources you may have to make required changes, and the potential difficulty of replacing the system or piece of equipment in question.

Once you have identified all safety-related systems and equipment that may be vulnerable to date-change failure and defined the necessary work to make them Y2K compliant, move on to assessing the effect of each item on safety in your facility and setting priorities for making necessary

corrections ***(see Appendix B)***.

Step 2 - Correction

The second step in the process is to use the priorities set during the assessment part of the process, decide whether to repair, replace/retire, or work around the vulnerable safety-related systems and equipment that you inventoried. Numerous diagnostic tools are available to assist you with these decisions. Many can be accessed on the Internet. ***Appendix C*** contains information about these and other resources.

In some cases, selecting a remedial approach will be straightforward. For example, installing a readily available software patch might be all that is necessary to solve a specific problem. These decisions can be much more difficult, however, if repair or replacement is expensive and the likelihood of failure cannot be clearly assessed.

When selecting a remedial option, you may want to employ an approach similar to that used in prioritizing your inventory. The exception would be adding cost of remediation as an additional consideration. This includes weighing the following:

- The likelihood of failure
- The potential impact of failure - Will failure seriously hinder emergency response? Will it hinder day-to-day operations? Are redundant external resources available for response in the event of internal resource failure?
- The cost of remedial action -Consider both money and time required

Simple scoring methods (scales of 1 to 3, or 1 to 5) may be helpful in allocating limited resources. High-consequence, high-likelihood events deserve more attention and resources than high-consequence, low-likelihood events. This type of scoring can help to determine whether the best option is to repair, replace, or work around the particular system or piece of equipment.

Repair - For many systems (databases, custom computer applications), repair will require upgrading system code as well as data. For embedded Y2K problems, the repair may be as simple as replacing a chip set or circuit board. In some cases, however, due to cost, the availability of parts or the difficulty with accessing equipment, repair may not be an option. In all cases, you should mark the equipment for its Y2K status.

Replace - Systems and equipment of only marginal benefit should be retired if they are not Y2K compliant. Exercise caution when choosing to retire systems and equipment. Plan to retire them well before December 31, 1999. The absence of certain systems or equipment may demonstrate that they are more important than your assessment suggested. Taking them out of service early leaves time to reverse that decision and take whatever steps are possible to make them Y2K compliant.

Step 3 - Testing/Validation

The third step in the process is to test the ability of repaired and replacement systems, including interactive systems, to function using Y2K rollover conditions in the real environment or in a realistic simulation. The risks of system failure should be assessed

before undertaking tests. Testing schedules should include allowances for dealing with such failures and any resulting additional remediation work and re-testing in order to minimize the impact of any failure.

Conducting appropriate testing may require close coordination between personnel from different departments. Because of the importance of meeting deadlines for correcting priority systems and equipment, testing could cause production and other operational delays, and staff from all levels and disciplines already may be under pressure to minimize downtime. *Before you test, alert local emergency officials, and make sure your employees and community are prepared for any possible failures*.

Plan to conduct as much of the remediation and testing as possible in a non-operating environment. However, at some point, it will be necessary to put each safety-related system through a full check in its normal operating environment. These checks should be carefully controlled and monitored, and independent verification of tests may be appropriate in some cases.

To encourage Y2K testing, EPA has initiated an enforcement policy designed to encourage prompt testing of computer-related equipment to ensure that environmental compliance will not be impaired by the Y2K computer bug. Following this policy, EPA intends to waive 100% of civil penalties and recommend against criminal prosecution for environmental violations caused by tests designed to identify and eliminate the Y2K-related malfunctions. This policy is limited and subject to certain conditions. The Web site for the policy is referenced in ***Appendix C.***

Step 4 - Contingency Plan

The fourth step in the process is to develop contingency plans to manage unforeseen problems and emergencies involving each safety-related system and equipment. Among other things, these plans should address how systems would be manually operated or shut down until problems are resolved. Development of contingency plans should be undertaken simultaneously with the correction part of this process. Contingency plans should be revised, as needed, based on the results of the testing/validation part of the process. These plans should include consideration of staff requirements, particularly additional personnel that may be needed on-site if automated systems must be manually operated.

For the contingency plan to be workable, the people who are expected to implement the contingency plan need to be involved in its development. Efforts should begin with reviewing existing disaster and business continuity plans. Establish communications with suppliers. A good plan must consider Y2K failures of internal systems and with suppliers, customers, service providers, business partners and infrastructure service providers. For example, some scenarios to consider are the following:

- Key Source Raw Material Provider Cannot Deliver Materials
- Transportation Disruptions
- Equipment Failure
- Telecommunications Disruptions
- Power Failure
- Water and Sewer Service Interruptions
- Application Failure

You may need to determine which employees need to be on-site on January 1, 2000. Your contingency plan also should address failure of backup equipment and systems that also could be affected by Y2K problems. Consider the possibility that Y2K disruptions could potentially prevent police, fire and mutual aid assistance from arriving promptly or at all. Coordinate with your local emergency planning committee to ensure emergency response procedures and resources are adequate to cover possible Y2K consequences.

In some instances, additional staff training may be necessary to ensure that all relevant personnel are aware of the details of contingency plans and be able to implement them effectively. Once your Y2K contingency plan is developed, your facility needs to test it. When first tested, most plans have a major flaw. Correct problems identified through testing to ensure that your plan will be successful.

Other useful information on contingency planning can be obtained from the *Chemicals Information Technology Association Y2K Contingency Planning Guidelines* available on the Chemical Manufacturers Association Web site ***(see Appendix C).***

Remember, by finding failures early in 1999, you are more likely to get the help you need from vendors and local government and utilities than if you wait until crucial dates *(Appendix D)* when demand for support and help may be much greater.

.

Step 5 - Communications

The fifth step in the process is to communicate your facility's Y2K readiness or your activities to prepare for the Y2K event. Audiences for such information include your facility's employees, suppliers, vendors, customers, emergency response authorities, local government, and community organizations. Examples of this outreach may include facility tours, community meetings, Y2K readiness disclosures, communication with the Local Emergency Planning Committee (LEPC) or an emergency response practice drill. See ***Appendix E*** for suggestions about activities for specific audiences and communications.

Appendix A

CHECKLIST OF SYSTEMS AND EQUIPMENT POTENTIALLY VULNERABLE TO Y2K DISRUPTIONS IN A HYPOTHETICAL CHEMICAL PLANT

Component	Worst-case Failure Effects
Embedded Microchips	
Controllers	Inaccurate readings resulting in poor conversion
Weighers	
Reactor	
Charging	Wrong amounts reacting-poor conversion
Temperature	Poor conversion-explosion
Pressure	Poor conversion-explosion
Cleaning	Inaccurate timing-process interruption-release
Stripper	Contamination of product
Dryer	Water contamination of product
Centrifuge	Poor separation
Storage	Overflow release
Video Cameras	Failure to work
Still Cameras	Failure to work
Alarm Systems	Failure to work
Clocks	Show incorrect time
Elevators	Failure to work
Phones	Failure to work
Answering Machines	Failure to work
Heating/Ventilation/Air Conditioning	Failure to work
Fire Suppressions Systems	Failure to work
Software	
Mainframe, network, desktop, & communication computers	Data-generated errors may result in inaccurate data or system failures
Office computers	
Purchasing	No supplies
Inventory	Excess supplies
Distribution	Will issue incorrect orders
Sales	Will not be able to fill orders
Accounting	Will incorrectly compute
Personnel	Will not be correctly maintained
Process Computers	
Control	Explosion release
Transportation	Buildup of stock
Quality Control	Poor quality

Appendix A

CHECKLIST OF SYSTEMS AND EQUIPMENT POTENTIALLY VULNERABLE TO Y2K DISRUPTIONS IN A HYPOTHETICAL CHEMICAL PLANT (Continued)

Component	Worst-Case Failure Effects
Supply Chain	
Utilities	
Electricity	Process shutdown
Water	Process shutdown
Waste	Waste buildup beyond capabilities
Communications	No communication
Raw material suppliers	
Primary feedstock	Process shutdown
Initiator-catalyst	Process shutdown
Service providers	
Insurance	Extra expenses
Hospitals	No medical care
Vending	No food
Customers	No incoming funds
Security	
Video cameras	Failure to work
Security lights	Failure to work
Access	
Parking	Failure to work
Building	Failure to work
Room	Failure to work
Alarms	
Fire	Failure to work
Intrusion	Failure to work
Warning	Failure to work
Process	Failure to work

Note: *The information given in this table is provided as an* **example only**. *Checklists like this should be developed on an individual, plant-specific basis using criteria and knowledge that are unique to the plant.*

Appendix B

ASSESSING SYSTEM VULNERABILITY

Assessing relevance to safety

Safety is the overriding consideration for assessing your control systems for possible year 2000 problems. This Appendix provides a method for assessing whether or not your systems are
(a) safety and (b) date-dependent.

The following aspects should be considered when assessing the safety of a control system:

(a) Its contribution to safety, i.e., the importance of the system to maintaining safety (which is a function of how control systems are arranged to provide the required reduction in risk); and

(b) The consequences of its failure (the effects of a hazardous event).

The assessment sequence in Figure 1 (next page) is one of several methods for rating, on a scale of 0-3 (3 being the highest level), the contribution of a particular control system to the safety of your plant or process. Once you have determined the "contribution" of a system, estimate the "consequences" of its failure using the following rating scale:

(a) no consequences = **0**
(b) minor accident/reversible injury = **1**
(c) irreversible injury/loss of one life = **2**
(d) loss of many lives = **3**

Any system with a "consequence" rating of zero (0), should not be considered further. Assess the importance of each remaining system to safety by adding its "contribution" and "consequence" ratings. Its safety rating will be expressed on a scale of 2-6.

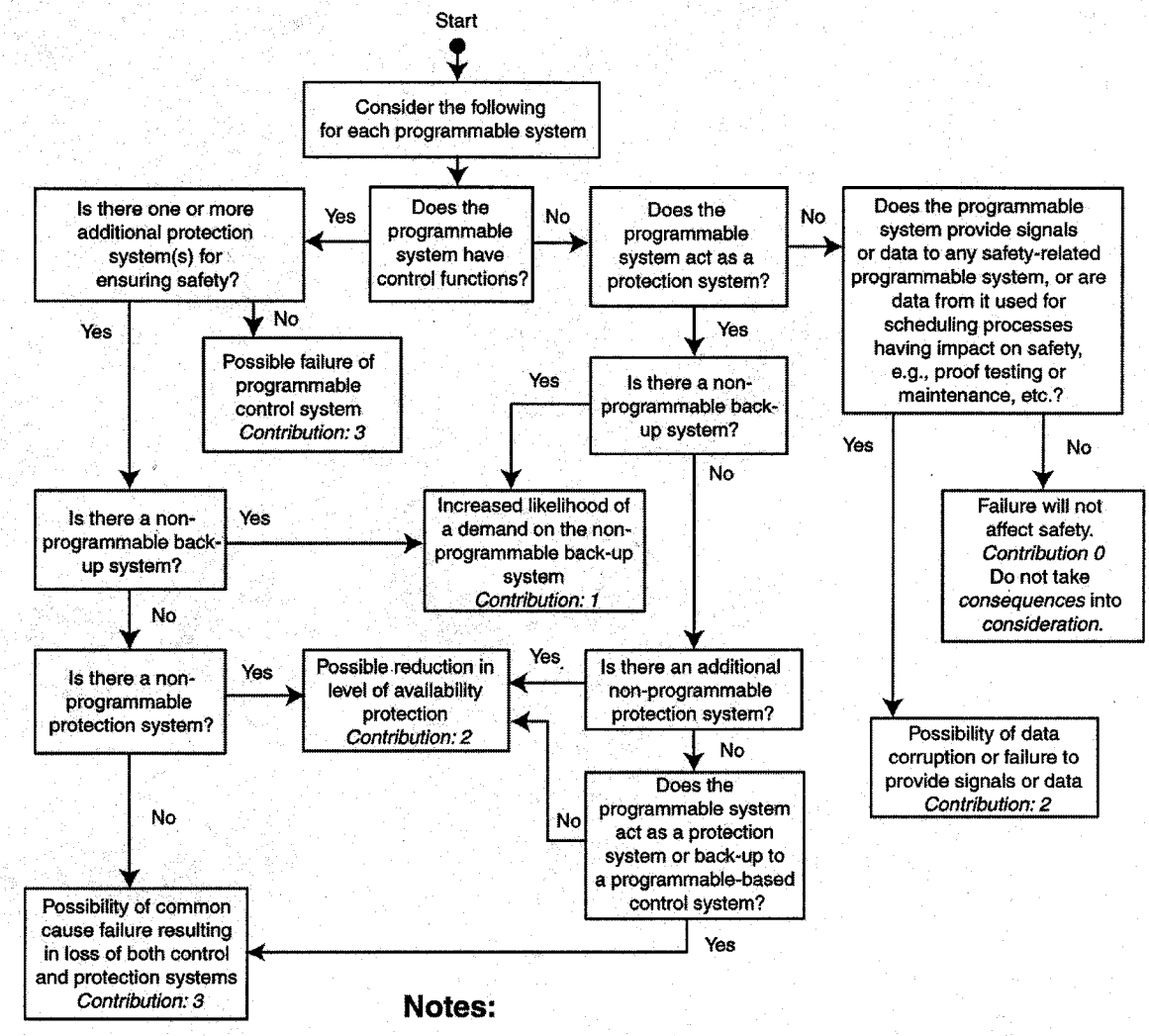
Assessing date dependency

Once the safety importance has been established, determine the date dependence of the system. Your employees may be the best source for obtaining this information.

The date-dependence checklist in *Figure 2* (page 3) is designed to assist you. Any YES answer indicates that the system has a potential date dependence that will require further investigation. **Even if all answers recorded are NO, it is strongly recommended that you confirm, through further investigation, that systems with a high safety importance are not date-dependent.**

Some systems, particularly "embedded" systems, may have date dependence that is not obvious. This "hidden" date dependence may affect other functions of the system. For example, printer output usually is date-stamped, so the presence of a printing option may introduce date dependency even if the printing option is not used.

Figure 1: Criticality Assessment



Notes:

1. This method is intended only as an aid to developing the priority order in which systems will be subjected to further investigation. It assumes that the risk reduction is spread evenly across all the safety-related systems.

2. The exception to the assumption in #1 is a back-up system that is capable of providing the full risk reduction in its own right.

3. In cases where the actual risk reduction is known, a more refined prioritization may be more appropriate.

Figure 2: Date dependence Checklist

Date Dependence Does the system:	**Yes**	**No**
Display or print a date or time?		
Implement a time control sequence?		
Perform operations on a timed basis?		
Produce time reports (hourly/daily/weekly)?		
Calculate time-based totals, averages, rates, or trends?		
Time stamp its data, or use time-stamped data?		
Maintain historical records?		
Display or print data by time sequence?		
Generate alerts at predetermined intervals (such as when set or maximum safe running time has been exceeded)?		
Request the date when started/powered up?		
Know which day of the week it is by date?		
Send date and time information to other systems?		
Connect to or contain a time-transmission receiver?		
Connect to a network providing access to the date?		
Did a visiting service engineer set its date?		
Require adjustment to allow for Daylight-saving Time?		
Can a command or function allow the date to be set?		
Navigate or position itself automatically (such as receivers for Global Positioning System satellites)?		
Remember user-defined data or settings even after being turned off for a long period?		
Need to be connected to a computer-based terminal for maintenance?		
Does system have a lithium battery?		

Appendix C

INFORMATION RESOURCES

The following are some resources to help you get started in addressing the potential Y2K problem in your facility.

American Petroleum Institute
The site provides industry activities, company status reports, Y2K database, and technical links.
http://www.api.org/ecit/y2k/index.html

Case Study of One Chemical Manufacturer's Approach to Y2K Problem
http://www.dell.com/smallbiz/y2k/studies.htm#merisol

Chemical Manufacturers Association (CMA)
CMA has member Y2K survey results and Y2K Contingency Planning Guidelines and practices available. Scroll down to Y2K category. http://www.cmahq.com/cmawebsite.nsf/pages/newsinfo

Electronic Information Clearing House on Chemical Emergencies.
This site is provided by the Organization for Economic Cooperation and Development (OECD) Working Group on Chemical Accidents. It has Y2K tools and links to help industry including an OECD Manual, *The Year 2000 Problem: Risks and Solutions.* This site is aimed at small and medium-size enterprises. It includes a system for routing inquiries and information about Y2K and hazardous installations to contacts in government and industry who have had some experience in dealing with the problem. http://www.oecd.org/ehs/y2k/index.htm

Electronic Industries Alliance
This trade association representing the high-tech industry has a Web site that provides a knowledge base and information center. It provides information sharing with its members, the government and the public.
http://www.eia.org/y2k/default.htm

Embedded Industrial Control Systems and Y2K
http://www.compinfo.co.uk/y2k/scada.htm

Fire Alarm Systems and The Year 2000 Problem
This site provides reference system for assessing whether fire alarm equipment may have a Y2K compatibility problem. http://www.fireline.com/firealarmsystems/y2000firealarmsystems.html

Health & Safety Executive (UK)
The British HSE Web site offers several reports on the Y2K problem: *Health and Safety and the Y2K Problem-Guidance on Year 2000 Issues As They Affect Safety-Related Control Systems* and *Contingency Planning for a Safe Year 2000* and *Year 2000 Risk Assessment: Will You Come Through the Millennium Safely?*
http://www.open.gov.uk/hse/dst/2000indx.htm

Information Technology Association of America
The ITAA is a major trade association for the Y2000 software conversion. It's Year 2000 Home Page contains useful resources, publications, and guides. http://www.itaa.org/year2000/index.htm

Institution of Electrical Engineers (U.K.)
IEE has a report addressing embedded chips. *The Millennium Problem in Embedded Systems* on its Web site.
http://www.iee.org.uk/2000risk/

Manufacturing Marketplace
Has a Year2000 page with Q&As, news about manufacturing and Y2K, reports on Y2K issues such as contingency planning, supply chain, etc., and Y2K/industry issues chat transcripts.
http://www.manufacturing.net/y2k/

Mary Kay O'Connor Process Safety Center
The site has links to compliance status of some manufacturers' control systems. Click on Y2K information.
http://process-safety.tamu.edu

Mitre Corporation
The site provides information on Y2K Certification, Compliance, Solutions, Testing and Evaluations, Contingency Plans, Cost Estimation, Tools and Services. http://www.mitre.org/technology/y2k

National Fire Data Center
A basic system check that can help you determine if your organization's computer system is Y2K compliant is available on this Web site. http://www.usfa.fema.gov/y2k/y2kcom.htm

National Institute of Standards and Technology (NIST)
The site has links to free software tests, self-help tools and product compliance status databases for use in Y2Kassessment, testing, contingency planning and remediation. Information is provided for smaller manufacturers through the Manufacturing Extension partnership, a nationwide network of centers providing technical and business assistance to smaller manufacturers. Small manufacturing firms can call 1-800-MEP-4MFG.
http://www.nist.gov/y2k/

President's Council on Y2K Conversion
This site has a list of computer manufacturers' Y2K sites. http://www.Y2k.gov/java/product_compliance.html

National Bulletin Board for Year2000
Provides tools for analysis, conversion, and testing for Y2k problems. http://it2000.com/solutions/index.html

PC Test Results for Y2K Problems
http://www.hqisec.army.mil/y2kweb/y2kresults.html
http://www.nim.com.au/year2000/ye02001.htm#ye02004

Synthetic Organic Chemical Manufacturers Association (SOCMA)
The 1999 Chemical Industry Y2K Readiness Survey, U.S. Senate testimony, and Y2K resources for the industry are available. http://www.socma.com/y2k.html

Tava Technologies
Plant Y2K: A White Paper that Discusses the Significance of the Effect of the Millennium Bug (Y2K) on Process Control, Factory Automation & Embedded Systems in Manufacturing Companies.
http://www.tavatech.com/files/TAVA3_0.pdf

U.S. Chemical Safety and Hazard Investigation Board (CSB)
The CSB has sponsored a conference and report on the Y2K problem and the potential of accidental chemical releases. The site includes the full text of the report *Year 2000 Issues; Technology Problems and Industrial Chemical Safety* as well as useful chemical safety Y2K links. http://www.chemsafety.gov/y2k

U.S. Environmental Protection Agency (EPA)
Provides information on EPA's efforts to address the Year 2000 problem for Environmental Y2K Sectors. Included is Y2K guidance for wastewater systems (including a checklist of basic systems) and a flyer on waste management and the Y2K problem. http://www.epa.gov/year2000/

EPA's Y2K Testing Enforcement Policy
http://es.epa.gov/oeca/eptdd/ocy2k.html

EPA's Office of Solid Waste and Emergency Response Y2K information
http://clu-in.org/y2k.htm

EPA's Chemical Emergency Preparedness and Prevention Office (CEPPO) has Chemical Emergency Y2K alert and updated links. http://www.epa.gov/swercepp/y2k.htm

U.S. General Accounting Office
Guide: *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* has general principles for use by businesses as well as government agencies. http://www.gao.gov/special.pubs/bcpguide.pdf

U.S. National Institute of Occupational Safety and Health (NIOSH)NIOSH has Y2K case studies, a web forum, vendor list, and an equipment manufacturer directory. http://www.cdc.gov/niosh/y2k/y2k-hmpg.html

U.S. Occupational Safety and Health Administration (OSHA)
The OSHA has resources and links for addressing the Y2K Impact on Safety and Health.
http://www.osha-slc.gov/html/oshay2kpage.html

U.S. Small Business Administration (SBA)
This Web site offers information specific to helping small businesses address the Y2K problem. It provides a list of questions to help identify date-sensitive equipment. SBA also has an extensive list of links to major corporations that post their Y2K status online.
http://www.sba.gov/y2k/ Hotline: 1-800-U-ASK-SBA (1-800-827-5722)

Year 2000
The site has a list of Year2000 vendors and consultants.
http://www.year2000.com

Y2K Freeware and Shareware
http://www.aphis.usda.gov/y2k/wares.html

Year 2000 Embedded Systems Vendors, Associations, and Manufacturers
http://ourworld.compuserve.com/homepages/roleigh_martin/y2k_com.htm

All URL address were accurate as of 6/24/99.

Appendix D

IMPORTANT DATES TO CHECK FOR Y2K DISRUPTIONS

Date	Reason for Concern
08/21/1999	Global Positioning system date rollover may affect military, transportation, Geographic Information System, and Automatic Vehicle Locator.
09/09/1999	Programmers use 9/9/99 as an end of file or infinity. (Ninth day of the ninth month of 99th year).
12/31/1999	End-of-year baseline (to be used in rollover scenario).
01/01/2000	Date rollover.
01/02/2000	First 24-hour look back period.
01/03/2000	First work day.
01/10/2000	First date requiring full use of seven digits.
02/28/2000	Date prior to Leap Year (to be used in rollover scenarios).
02/29/2000	Leap Year 2000.
02/30/2000	Invalid date. Test to ensure that Leap Year logic is functioning.
03/01/2000	First valid date after Leap Year.
10/10/2000	First date requiring full use of eight digits.
12/31/2000	Some systems using Julian dates may not recognize the 366th day of the Leap Year.
01/01/2001	First date in 2001. Check rollover functions.

Appendix E

Communicating Your Facility's Y2K Activities

One of the most important ways that your facility can maintain a positive image in the eyes of your local community, government and customers is to communicate what your plant is doing, or has done, to prepare for the Year 2000 transition. The following is a brief list of suggested audiences and methods for communicating your Y2K activities.

Employees

Employee communication and involvement is an important component of a facility communications program. It's also a good first step to educating the local community on your plant's Y2K safety procedures because most employees live in the local community. Some suggested employee activities are the following:

- Roundtables with the plant manager
- Emergency planning training programs
- In-house newsletters
- Display Y2K Readiness Disclosure in common areas
- Reviewing Y2K contingency plans with employees at staff meetings
- Distribute Y2K information to employees
- Conduct lunch hour meetings
- Include employees in development of contingency plan

Local Community

Communicating that your facility is Y2K compliant, or working to become Y2K compliant, is important to maintaining public trust. You can communicateY2K activities in many ways, including the following suggestions:

- Join local groups (Chamber of Commerce, LEPC, City Public Works Board, neighborhood associations, etc.)
- One-on-one community meetings (door-to-door announcements/meetings)
- Conduct neighborhood meetings
- Conduct facility tours
- Visit local schools
- Attend town meetings
- Write public service announcements for local newspapers
- Develop and disseminate plant information sheets that include Y2K activities

Local Emergency Responders

Once you have developed a Y2K contingency plan, you should distribute it, along with any other emergency response plans, to the following groups and/or agencies:

- Department of Environmental Management
- County sheriff's department
- Local fire department/HAZMAT Team
- LEPC
- Local hospitals
- Local police department
- County civil defense organization
- Facility emergency team

You should also coordinate meetings and events with the local fire department and/or HAZMAT Team to review all critical procedures and on-site chemicals. Conducting a Y2K emergency response drill with local emergency responders will test your contingency plan and prepare all people involved.

Customers and Vendors

Letting your customers and suppliers know that you are actively preparing your facility for the Y2K conversion is an important business activity to ensure customer confidence and vendor rapport. The following are ways to communicate with this important group.

- Department of Environmental Management
- County sheriff's department
- Local fire department/HAZMAT Team
- LEPC
- Local hospitals
- Local police department
- County civil defense organization
- Facility emergency team

The Y2K Disclosure Statement

Once your company is Y2K compliant, perhaps the most effective and simple way to communicate this status is to prepare a Y2K disclosure statement. This document must be titled as a "Y2K Disclosure Statement" to avoid potential legal liability. A sample Y2K Disclosure Statement is below.

XYZ Chemicals
Y2K Disclosure Statement

Month/Date, 1999

Dear Customers and Suppliers:

As a trusted supplier of chemicals/suppliers, this disclosure describes XYZ Chemical's Y2K status to inform you of our preparedness as defined by the Year 2000 Information and Readiness Disclosure Act (15 USC 1 Note, PL 105-271). We have evaluated all of our machinery and equipment and have determined that there do not appear to be any issues that may affect our operations before, during or after the Year 2000. We have contacted and are actively dealing with all of our computer hardware and software vendors to continue our commitment of quality and service beyond the Year 2000.

When appropriate and important, efforts are being (have been) made to determine if other relevant third party vendors, suppliers and service providers beyond XYZ's control, also are actively engaged in achieving Y2K compliance in their products, services and general corporate viability, whichever may apply.

I hope this disclosure satisfies any concerns you have regarding XYZ Chemical's Y2K readiness. If you have any questions, please call me at (000) 555-1234.

Sincerely,
John Doe
Title